



FIG. 1  
(PRIOR ART)

PLAIN TEXT

Application No. 09/879,793

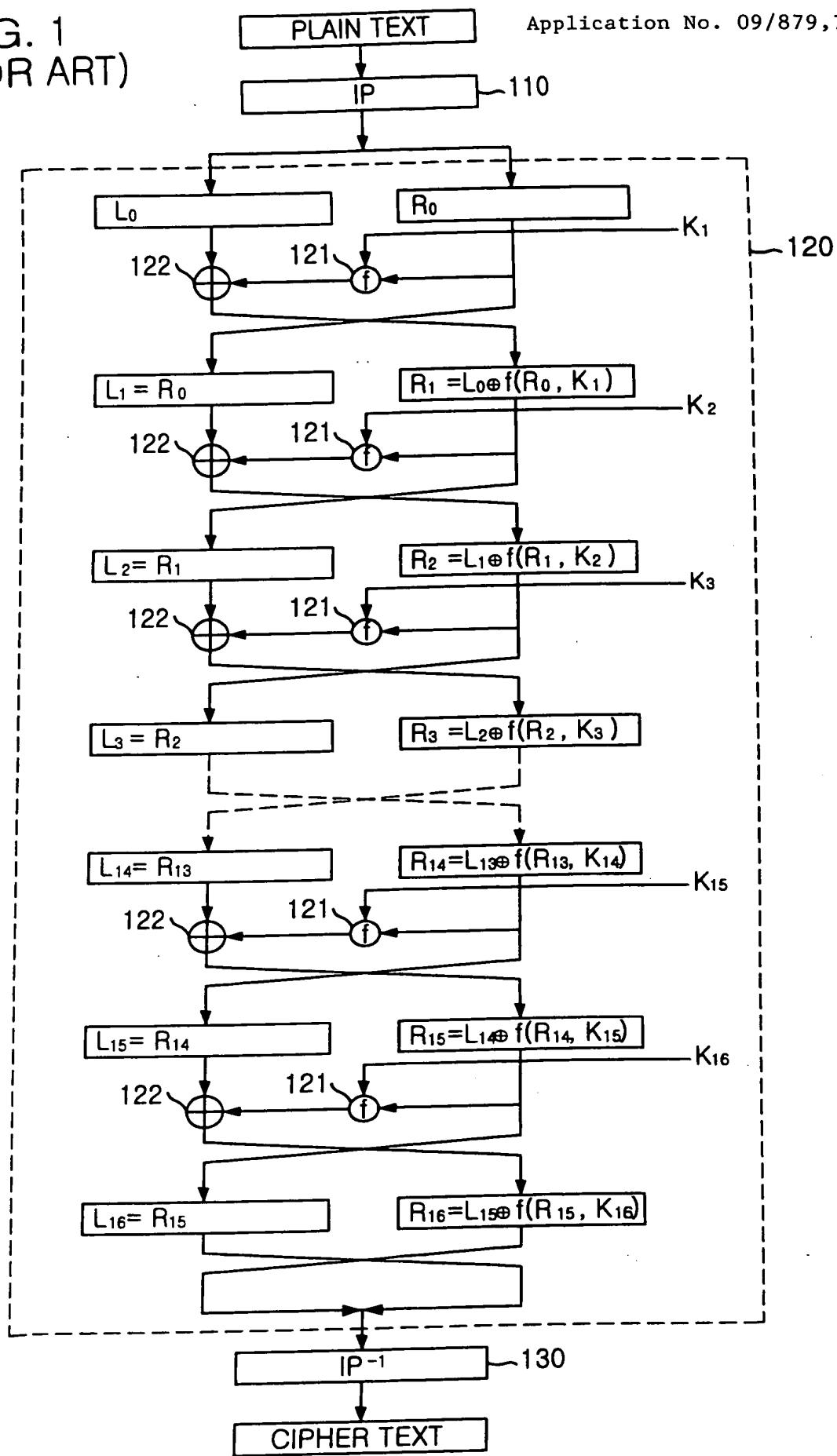


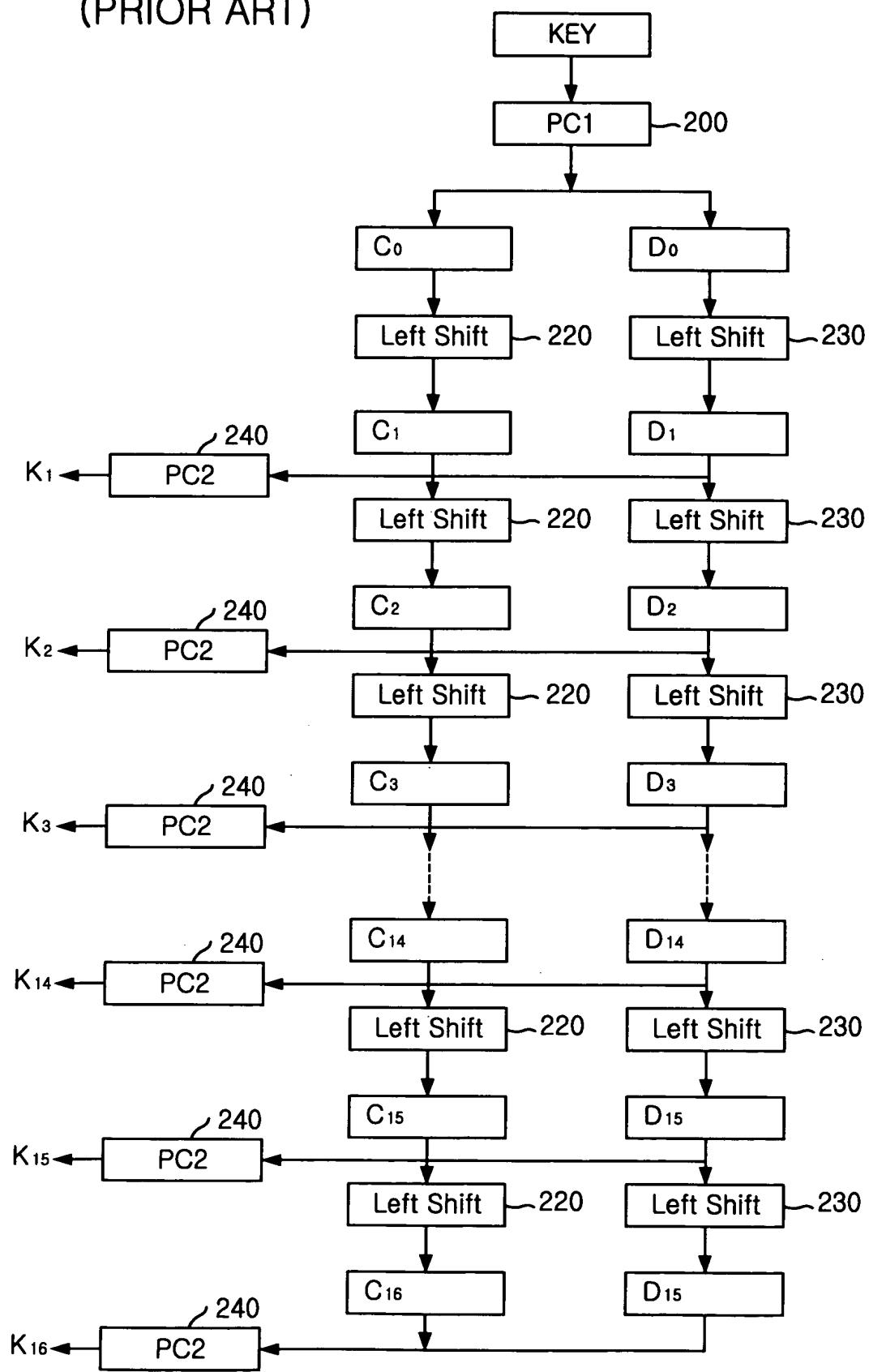
FIG. 2  
(PRIOR ART)

FIG. 3  
(PRIOR ART)

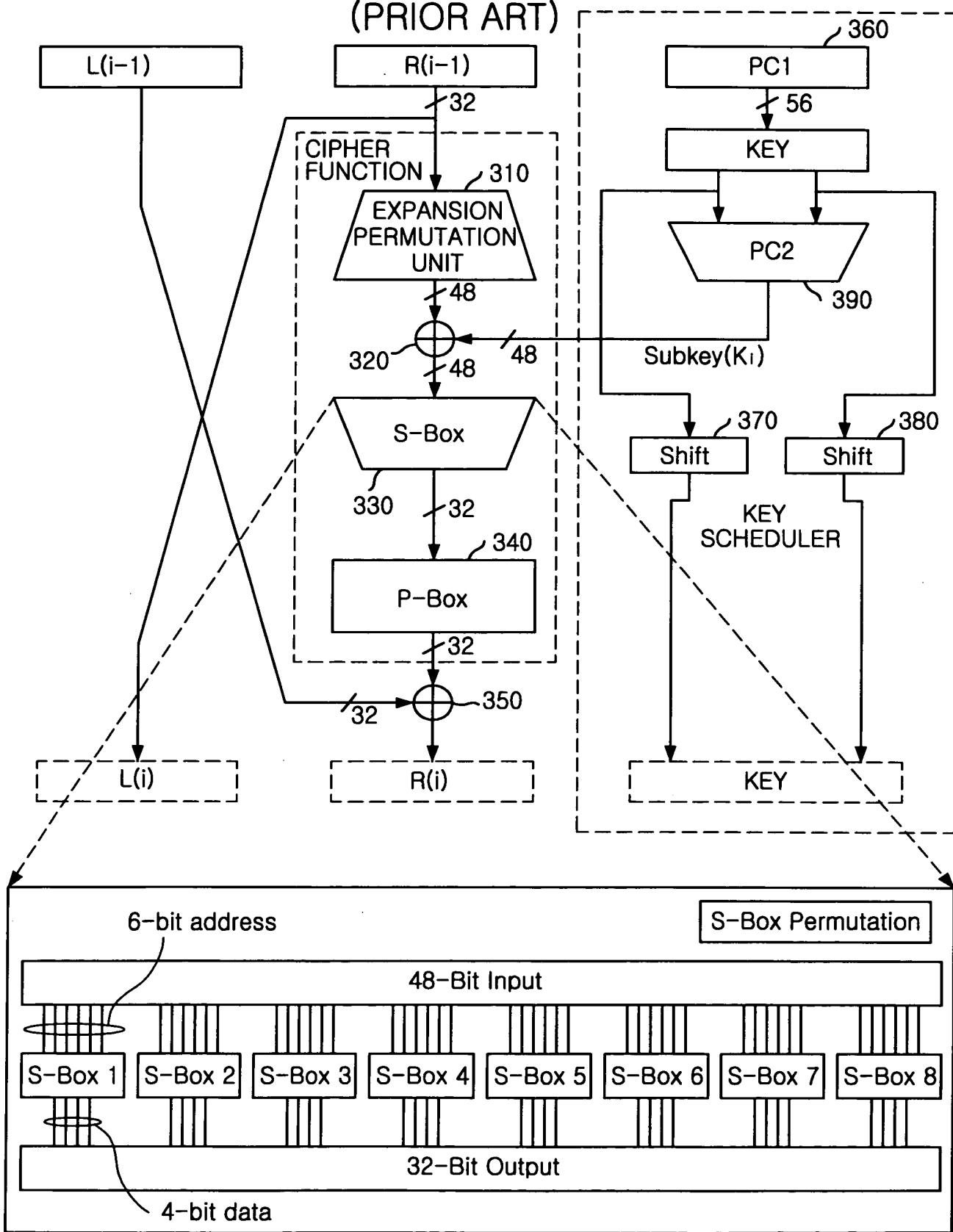




FIG. 4  
(PRIOR ART)

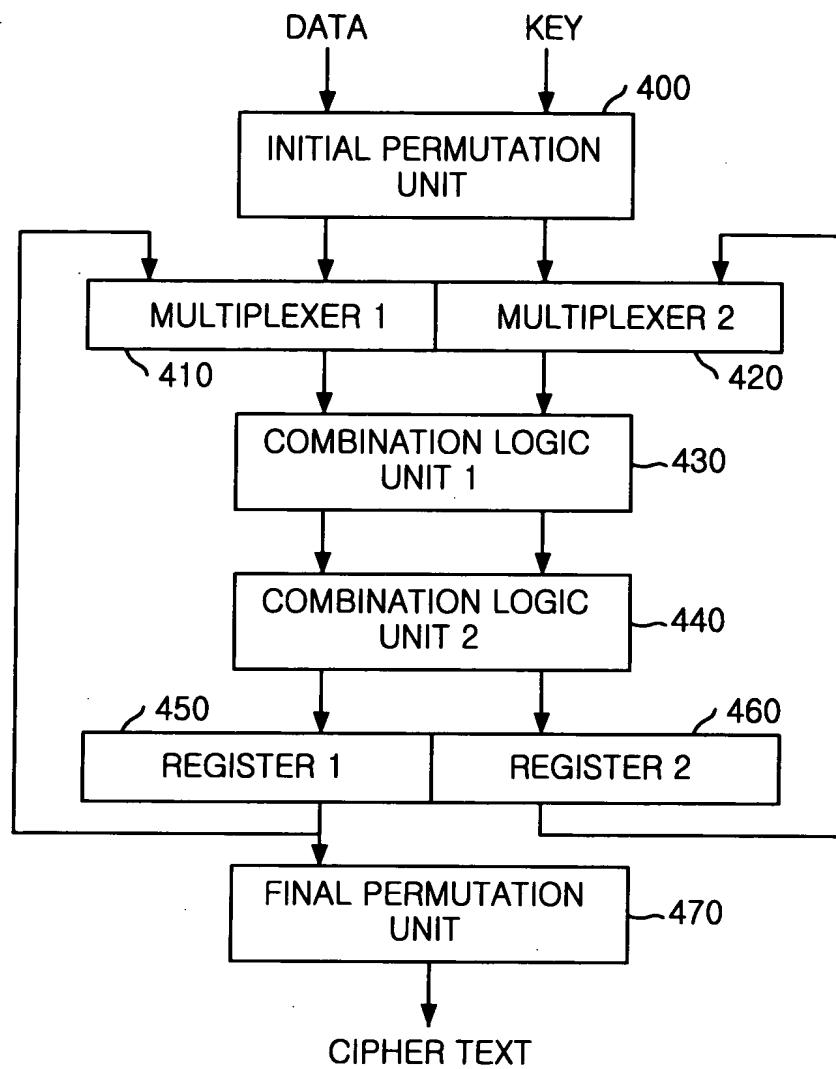
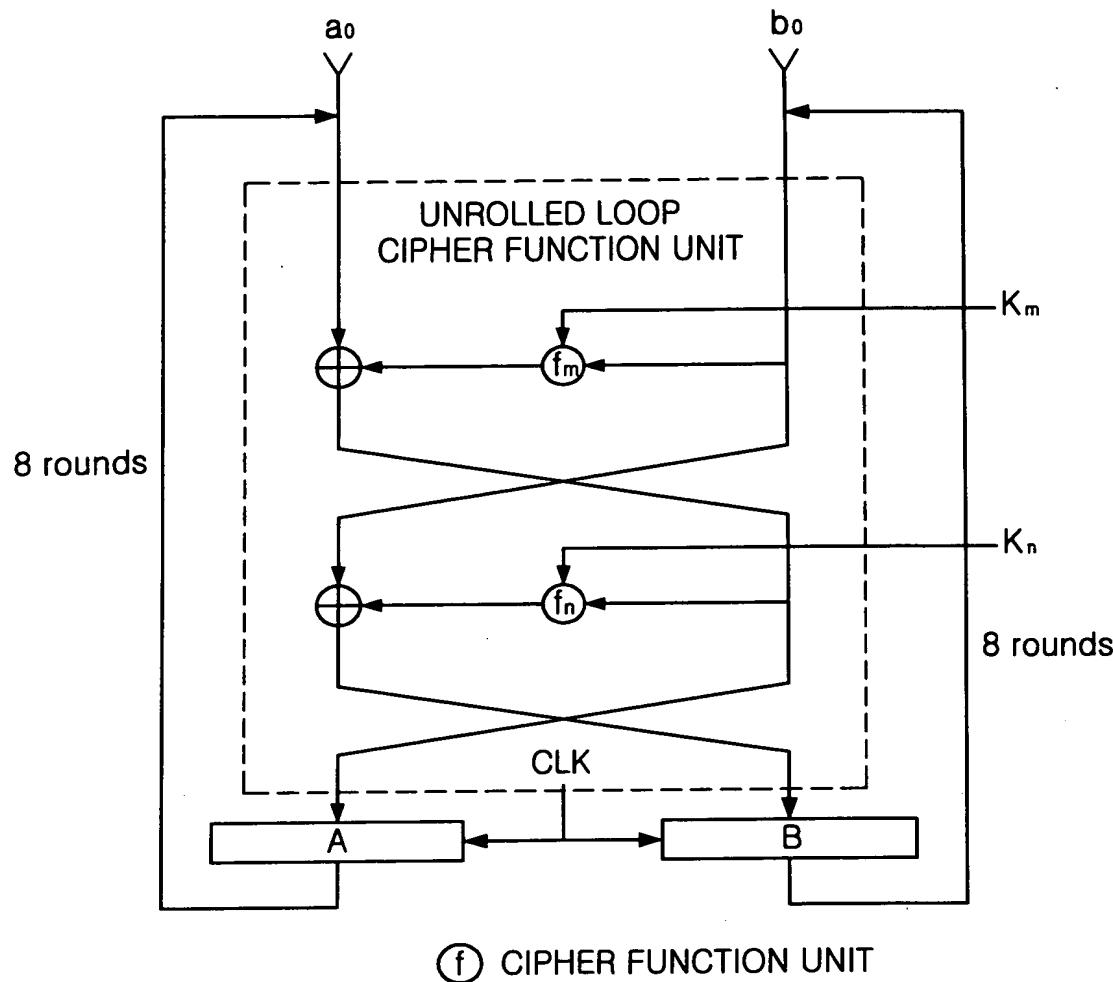




FIG. 5A  
(PRIOR ART)





Application No. 09/879,793

FIG. 5B  
(PRIOR ART)

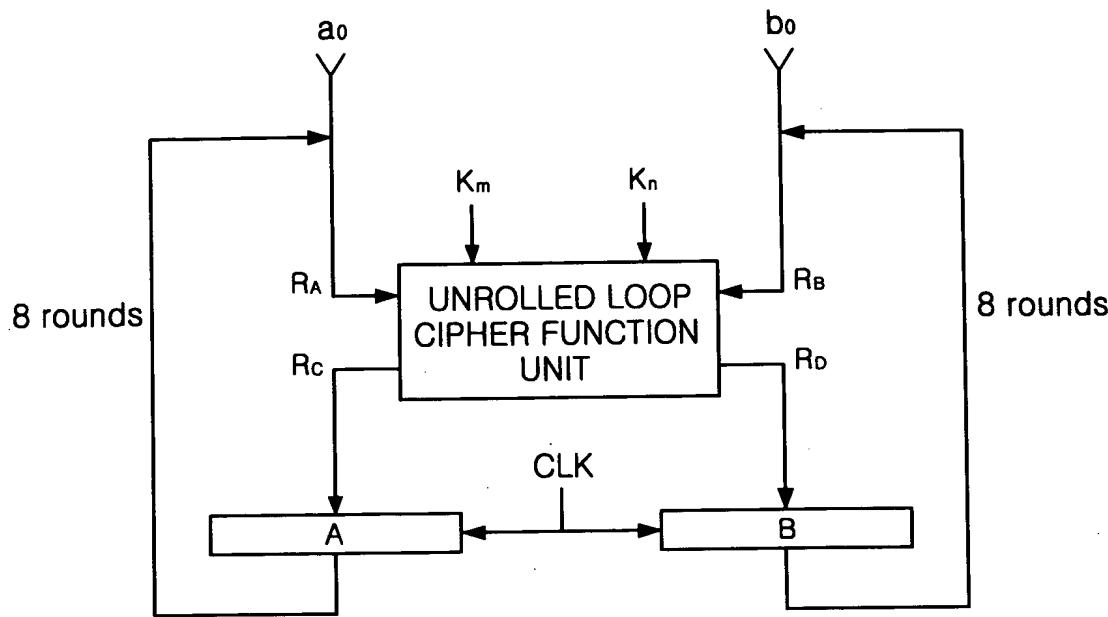




FIG. 6  
(PRIOR ART)

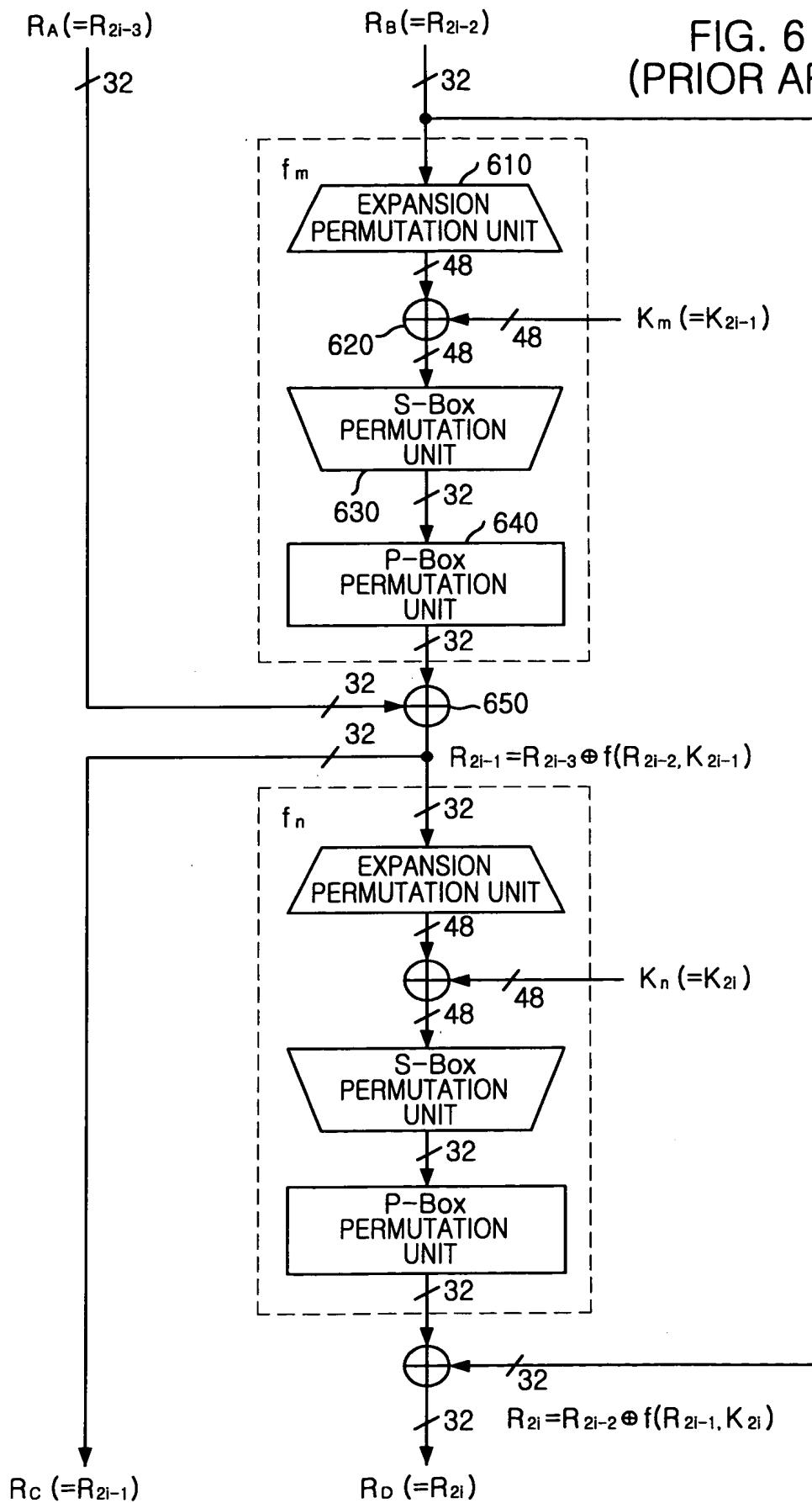




FIG. 7  
(PRIOR ART)

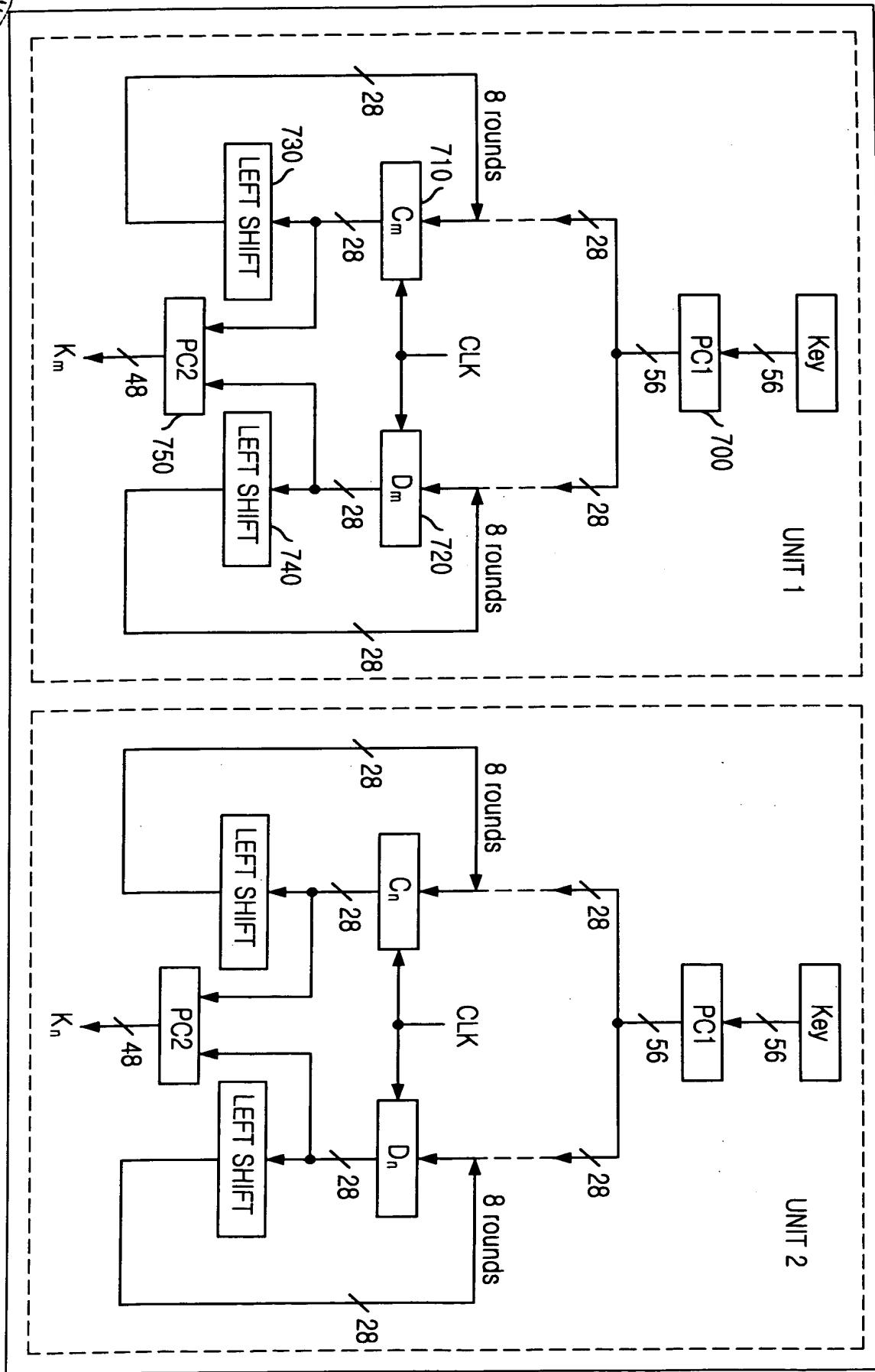




FIG. 8

Round	$S_m$	$TS_m$	$D_m$	$TS_n$
1( $P_0$ )	3	1	+1	2
2( $P_1$ )	4	4	+2	6
3( $P_2$ )	4	8	+2	10
4( $P_3$ )	3	12	+2	14
5( $P_4$ )	4	15	+2	17
6( $P_5$ )	4	19	+2	21
7( $P_6$ )	4	23	+2	25
8( $P_7$ )	$2*(1)$	27	+1(0)	0

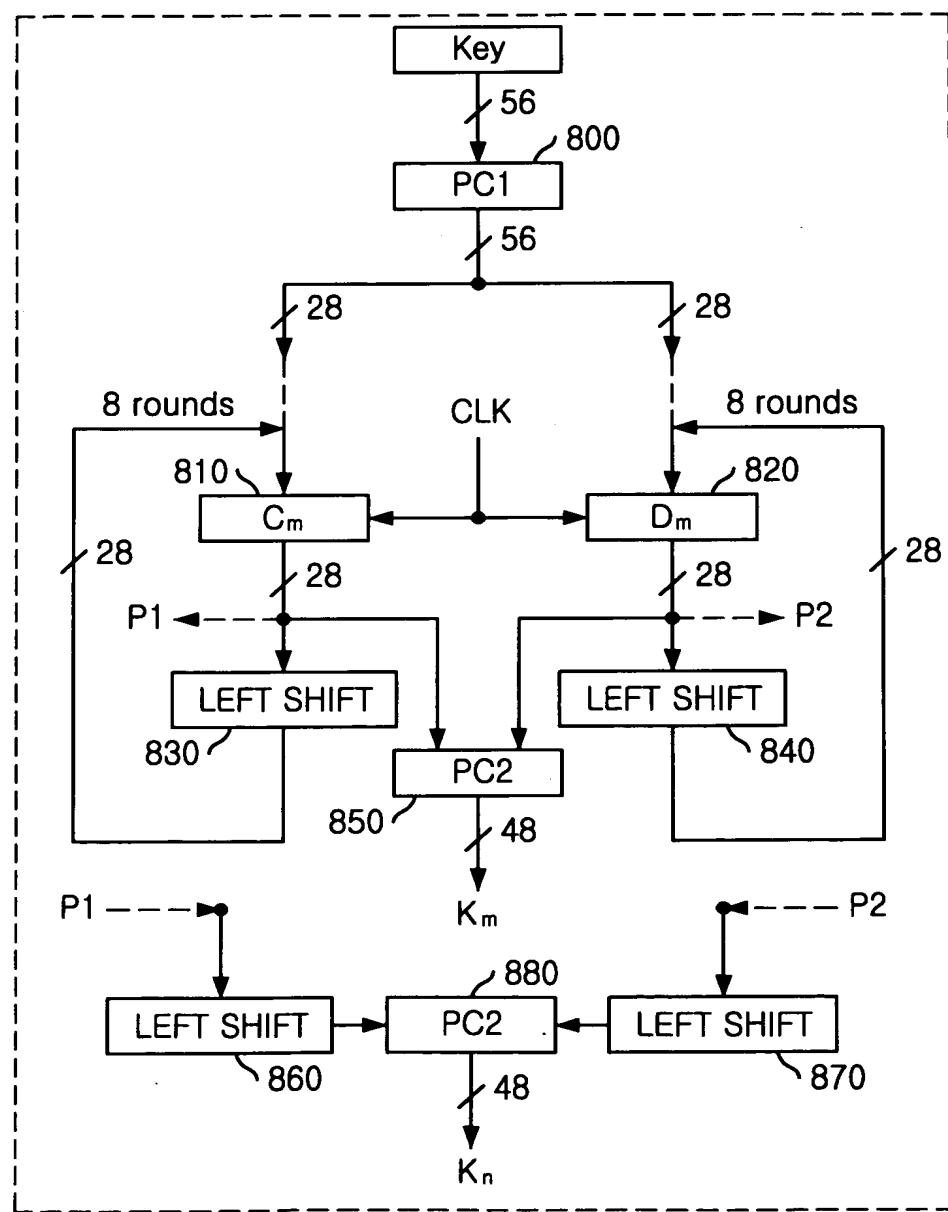




FIG. 9

Round	$S_n$	$TS_n$	$D_n$	$TS_m$
1( $P_0$ )	4	2	-1	1
2( $P_1$ )	4	6	-2	4
3( $P_2$ )	4	10	-2	8
4( $P_3$ )	3	14	-2	12
5( $P_4$ )	4	17	-2	15
6( $P_5$ )	4	21	-2	19
7( $P_6$ )	3	25	-2	23
8( $P_7$ )	2	0	-1	27

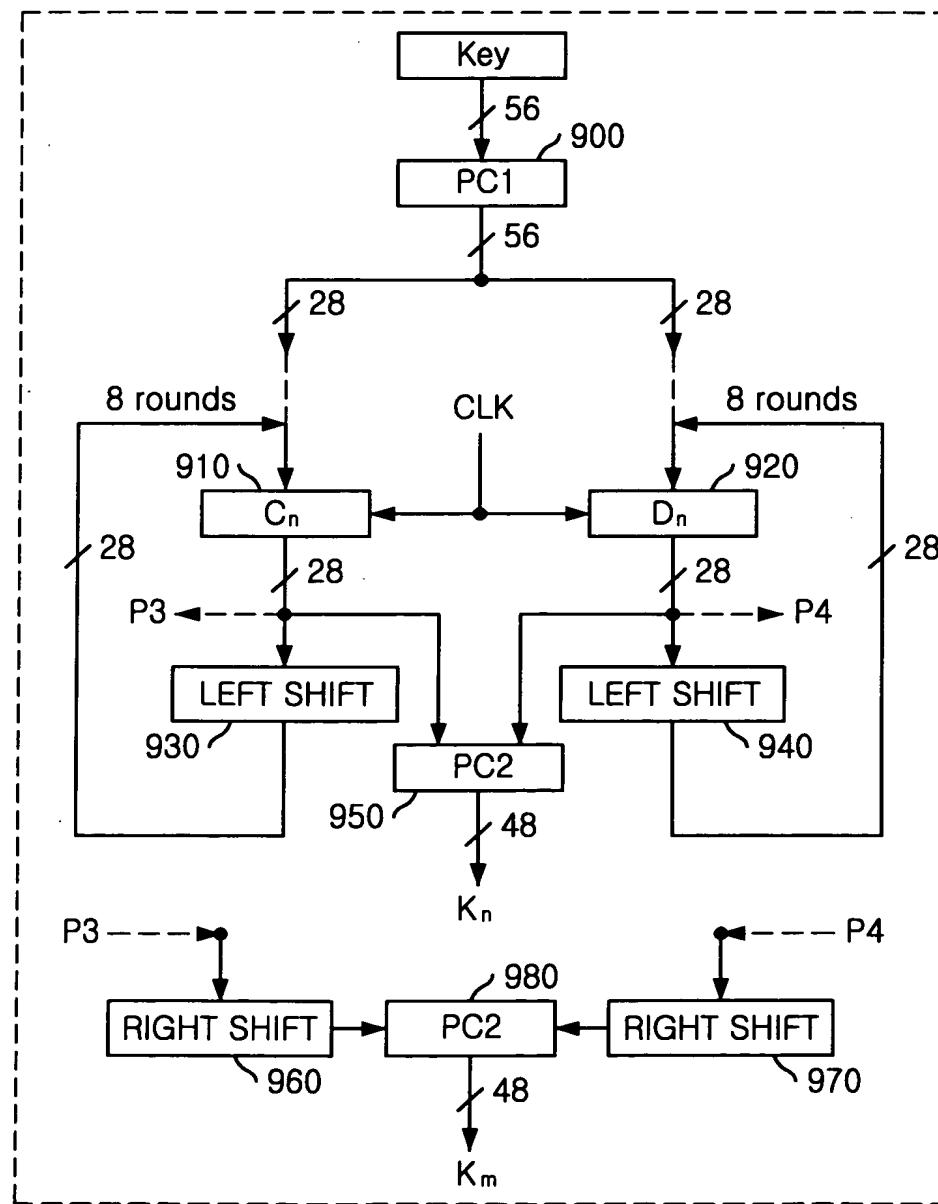




FIG. 10

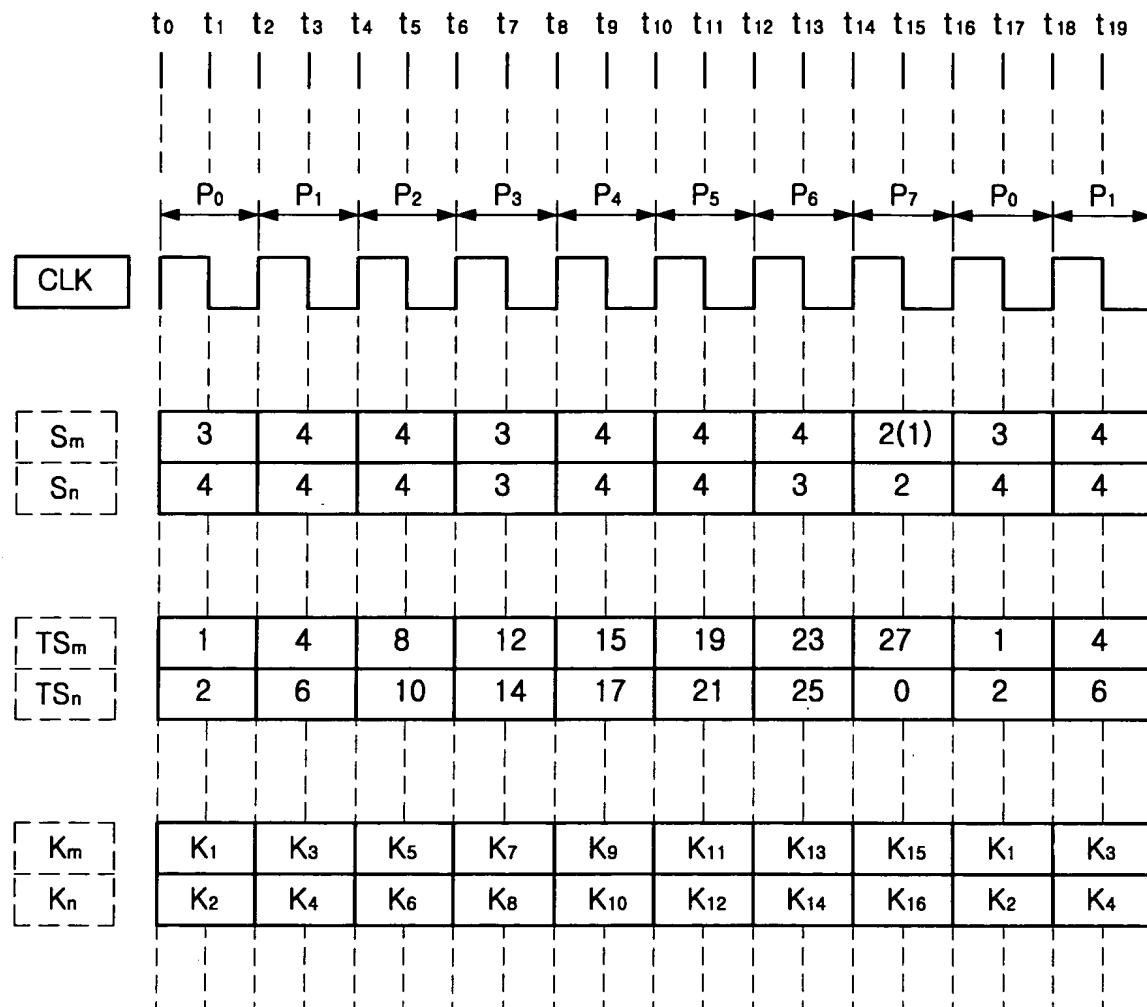




FIG. 11

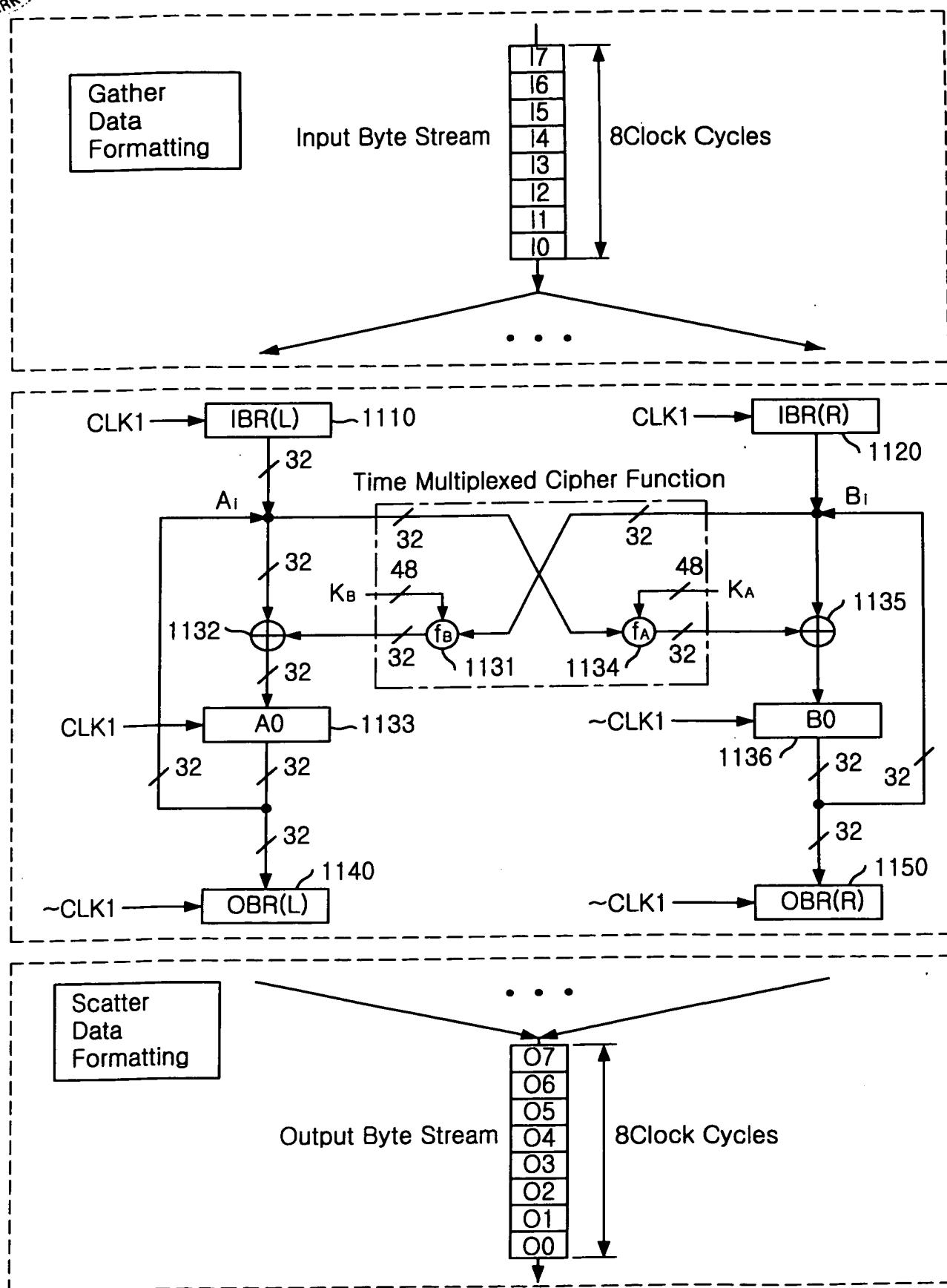
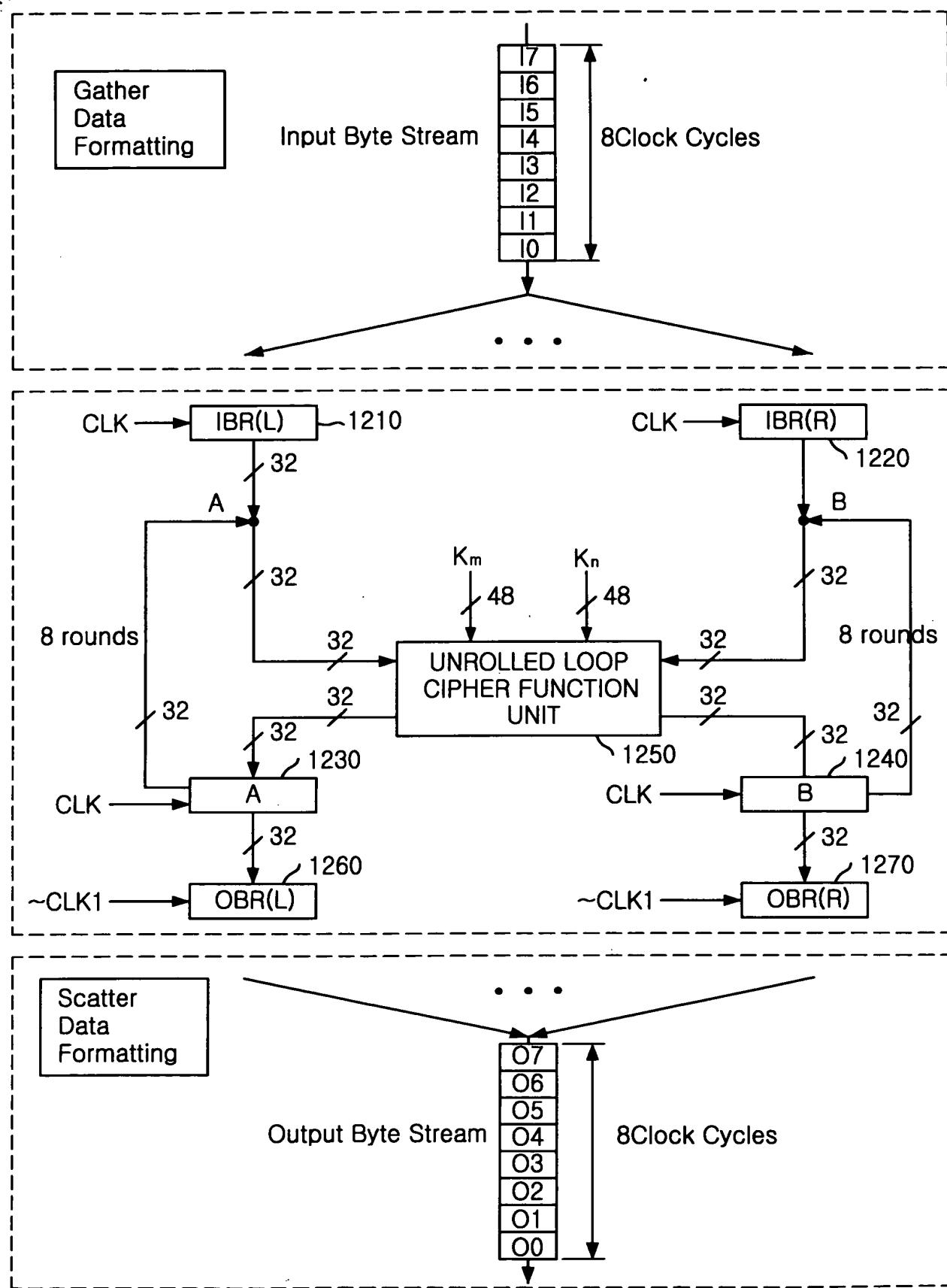




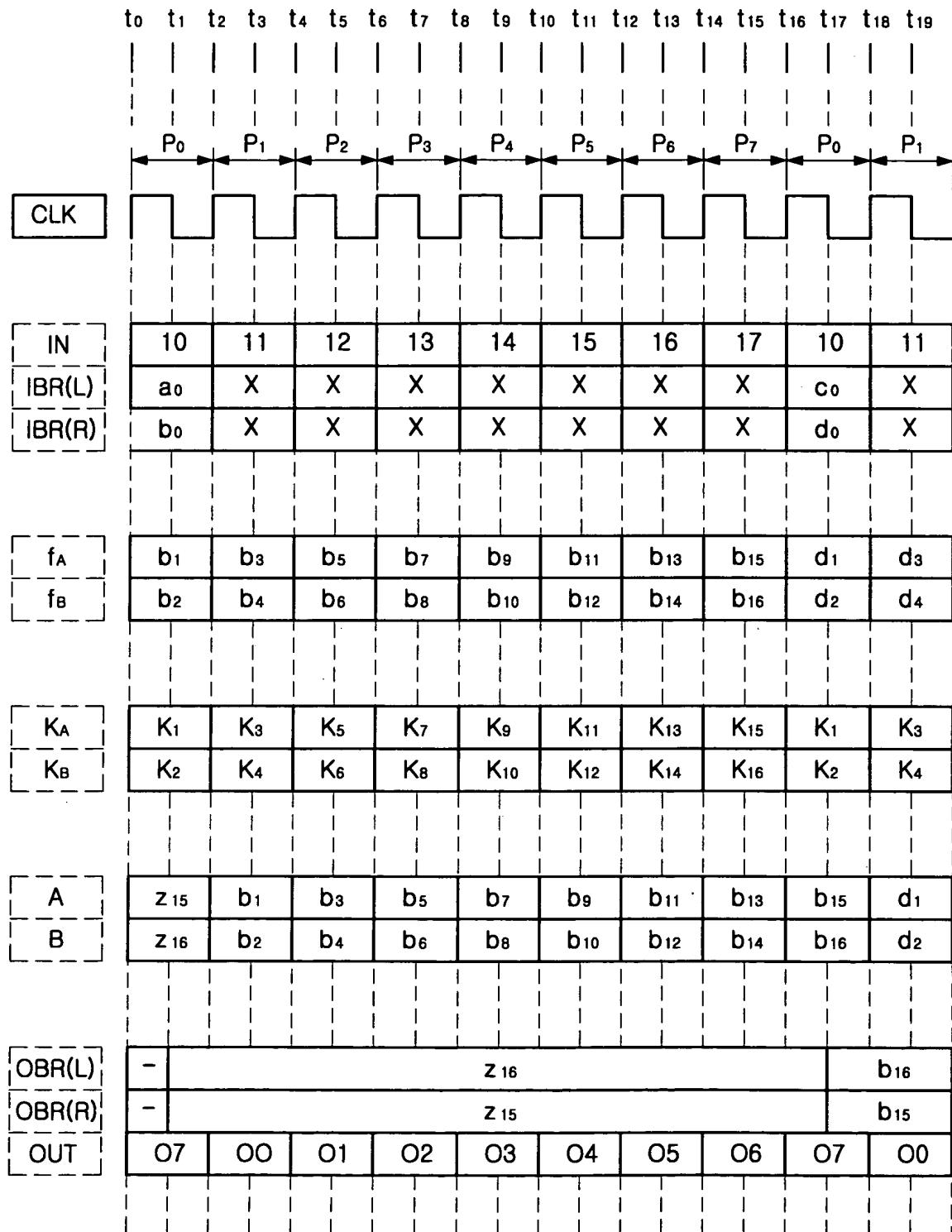
FIG. 12



JUN 01 2005

PATENT &amp; TRADEMARK OFFICE

FIG. 13



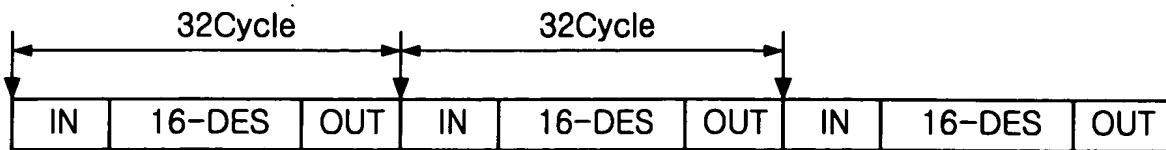
JUN 01 2005



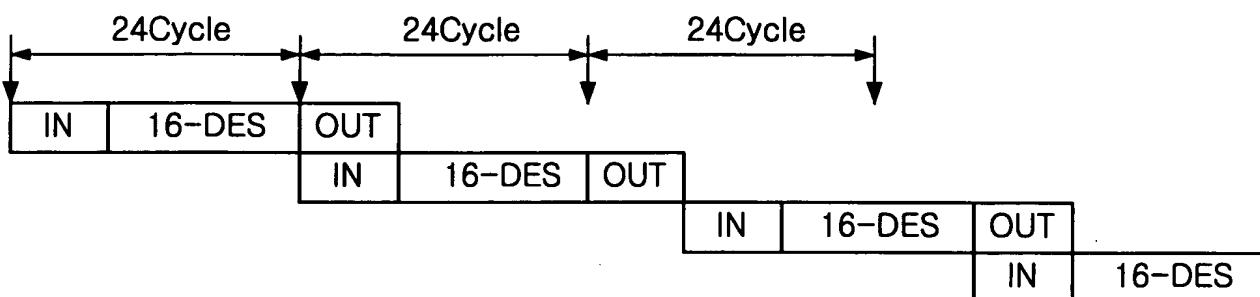
FIG. 14

## Traditional 16 Round DES

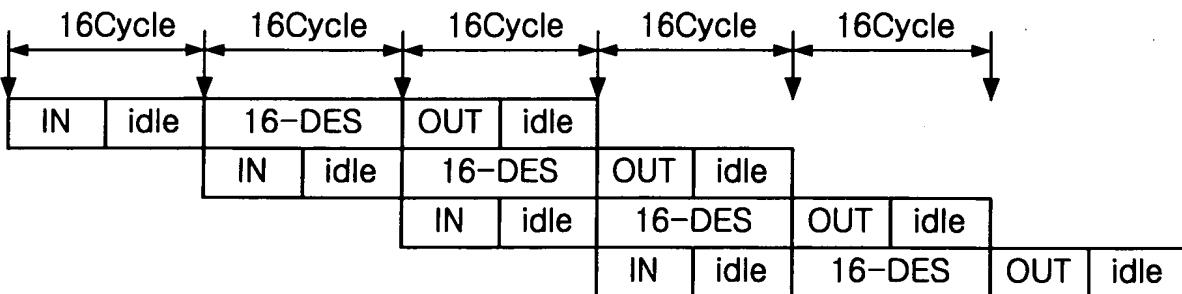
(1) No Latency Hiding (Latency=32, Throughput=1/32)



(2) 2-Stage Macro Pipeline (Latency=32, Throughput=1/24)



(3) 3-Stage Macro Pipeline (Latency=40, Throughput=1/16)



## 8Round DES (Loop Unrolled Cipher function &amp; Time Multiplexed Cipher Function)

(4) 3-Stage Macro Pipeline (Latency=24, Throughput=1/8)

